Journal of Law and the Biosciences, 1–21
doi:10.1093/jlb/lsaa034
Advance Access Publication 28 May 2020
Original Article

COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes

Laura Bradford*,†, Mateo Aboy and Kathleen Liddell

Centre for Law, Medicine and Life Sciences (LML), Faculty of Law, University of Cambridge, Cambridge, UK
*Corresponding author. E-mail: lrb45@cam.ac.uk

ABSTRACT

Digital surveillance has played a key role in containing the COVID-19 outbreak in China, Singapore, Israel, and South Korea. Google and Apple recently announced the intention to build interfaces to allow Bluetooth contact tracking using Android and iPhone devices. In this article, we look at the compatibility of the proposed Apple/Google Bluetooth exposure notification system with Western privacy and data protection regimes and principles, including the General Data Protection Regulation (GDPR). Somewhat counter-intuitively, the GDPR's expansive scope is not a hindrance, but rather an advantage in conditions of uncertainty such as a pandemic. Its principle-based approach offers a functional blueprint for system design that is compatible with fundamental rights. By contrast, narrower, sector-specific rules such as the US Health Insurance Portability and Accountability Act (HIPAA), and even the new California Consumer Privacy Act (CCPA), leave gaps that may prove difficult to bridge in the middle of an emergency.

KEYWORDS: COVID-19, tracking app, GDPR, HIPAA, CCPA, privacy and data protection, OECD privacy principles

† Laura Bradford is a Senior Research Associate in the Centre for Law, Medicine and Life Sciences (LML) at the University of Cambridge, UK, where she also teaches US Corporate Law in the Masters in Corporate Law (MCP) program. She is dual qualified as a Solicitor in the UK and an Attorney in New York. For the past 3 years, she has served as a Senior Legal Advisor for the University of Cambridge, UK. In the USA, she was an Assistant Professor at George Mason University Law School and a Visiting Associate Professor at George Washington University School of Law. She graduated with honors from Stanford University Law School and Yale University.

INTRODUCTION

Digital surveillance and tracking has played a crucial role in containing the Coronavirus outbreak in China, Singapore, and South Korea, among others.[1] On April 10, Google and Apple announced a joint effort to enable public health authorities to build applications to perform contact tracing using iPhone and Android devices.[2] The collaboration between government agencies and Silicon Valley tech giants immediately raised privacy concerns. Whether large-scale tracing of exposure can coexist with more stringent legal protections and norms for individual privacy and autonomy prevalent in Europe and the USA is unclear. Some may even be tempted to suspend data protection mandates in a state of emergency.[3] The need to track individual movements and health status on a broad basis offers a crucial 'stress test' of Europe's nascent, comprehensive General Data Protection Regulation (GDPR) and other privacy and data protection regimes based on OECD Privacy Guidelines.[4]

In this article, we look at the compatibility of the proposed Apple/Google Bluetooth exposure notification system ('ENS') and associated applications with Western privacy and data protection principles, including the EU GDPR. Depending on their final details, and how they develop over time, our view is that the Apple/Google ENS will fall within the governance system of the GDPR and, along with associated software applications, can be operated in a way that is compatible with the GDPR rules. In contrast, substantial parts of the Apple/Google ENS and any associated applications may fall outside data protection laws in the USA. As a consequence, uptake of such systems by health agencies and citizens may prove slower. Narrower, sector-specific rules such as the US Health Insurance Portability and Accountability Act (HIPAA), and even the new California Consumer Privacy Act (CCPA), leave gaps that may prove difficult to bridge in the middle of an emergency. Thus, somewhat counter-intuitively, the GDPR's expansive scope is not a hindrance but rather an advantage in conditions of uncertainty such as a pandemic. The GDPR framework offers a comprehensive, functional blueprint for digital system design that is compatible with fundamental

1 *Euronews, Coronavirus Conundrum: COVID-19 Tracking Apps That Do Not Breach Privacy* (television broadcast, Apr. 9, 2020), https://www.youtube.com/watch?v=_goD-J96br0&feature=youtu.be; *see also* Jennifer Valentino-DeVries, *Translating a Surveillance Tool into a Virus Tracker for Democracies*, NY Times, Mar. 19, 2020.

2 Press Release, Apple, Apple and Google Partner on COVID-19 Contact Tracing Technology, https://www.apple.com/uk/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ (accessed Apr. 10, 2020).

3 *See, eg* Samuel Stolton, *EU Watchdog Very Worried by Hungary's GDPR Suspension*, EURACTIV, https://www.euractiv.com/section/data-protection/news/eu-data-watchdog-very-worried-by-hungarys-gdpr-suspension/ (accessed May 18, 2020); Stewart Baker, *The Problem with Google and Apple's COVID-19-Tracking Plan*, Lawfare, Apr. 14, 2020 (advising that US state governors use emergency powers to order Google and Apple to build interfaces that privilege stopping the virus over privacy concerns); Anindya Ghose & Daniel D. Sokol, *Unlocking Platform Technology to Combat Health Pandemics*, Yale J. on Reg. 3 (2020) (advising the creation of a set of mandatory data sharing exceptions to allow platforms to harness individual personal data for public health purposes), https://ssrn.com/abstract=3580947.

4 The OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980 constituted the first internationally agreed upon set of privacy principles. Organisation for Economic Cooperation and Development [OECD], *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980) C(80)58/FINAL 1980) [hereinafter *OECD Guidelines*], https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, *revised as* OECD Privacy Framework 2013, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

rights. Indeed, it is clear that GDPR's Article 5 core principles were very much front of mind for the two technology companies as they designed their new interfaces.[5]

WHAT DATA IS BEING COLLECTED?

Many, if not all, EU countries are currently working on applications ('apps') aimed at facilitating the fight against the COVID-19 crisis. Some of them are based on geolocation, such as Coronamadrid and StopCovid19 in Spain, whereas others are based on the Bluetooth technology known as a 'digital handshake', such as Stopp-Corona-App in Austria, StopCovid in France, ProteGo in Poland, or an app being developed by the National Health Service ('NHS') in the UK.[6] The Apple/Google ENS enables interoperability between Android and iOS devices and apps to permit tracking using Bluetooth technology of 'contact events' between devices. [7] Apple/Google have stated that only apps designated by public health authorities will have access to this framework and such apps must meet specific criteria around privacy, security, and data control.[8]

The Google/Apple ENS allows iPhone or Android devices to detect other devices that have been within a certain distance for a significant duration. That 'handshake' will cause unique identifier codes to be stored, in encrypted form, on both devices.[9] If someone subsequently tests positive for the virus, that person will upload information centrally to an app server together with their unique identifier codes. The ENS will download positive diagnosis identifier codes daily and will match them with codes stored on individual devices. A match will generate an automatic notification from the app, which will appear on any device that recorded the infected individual's device identifier(s) during the relevant time period. Information about exposure events largely stays on each user's phone, while the central server and ENS process only 'de-identified' information about individuals with a positive diagnosis.[10] In the coming months, Apple and Google will work to enable a broader Bluetooth-based ENS by building the

5 *Eg* Press Release, Apple *supra* note 2 (stating that user privacy and security were central to the design of their APIs); Zach Whitaker & Darrell Etherington, *Q&A: Apple and Google Discuss Their Coronavirus Tracing Efforts*, TECHCRUNCH, https://techcrunch.com/2020/04/13/apple-google-coronavirus-tracing/ (accessed Apr. 13, 2020) (describing the service as 'privacy-focused').

6 Christian Runte *et al*, *Is a Privacy-Friendly Use of Mobile Applications to Combat COVID-19 our Exit Plan from the Crisis?* CMS Law Now, https://www.cms-lawnow.com/ealerts/2020/04/is-a-privacy-friendly-use-of-mobile-applications-to-combat-covid19-our-exit-plan-from-the-crisis?cc_lang=en (accessed Apr. 17, 2020).

7 Press Release, Apple *supra* note 2.

8 Apple/Google, Exposure Notification: Frequently Asked Questions v. 1.1, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf (accessed May 3, 2020) [hereinafter FAQ].

9 This involves detection and storage of rolling device identifiers during each specified contact event. See Apple/Google, Contact Tracing Bluetooth Specification v. 1.2, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf; (accessed Apr. 2020) [hereinafter Bluetooth Specification]; *see also* Whitaker & Etherington, *supra* note 5; Privacy International, Bluetooth Tracking and COVID-19: A Tech Primer, https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer (accessed Mar. 31, 2020); Andy Greenberg, *Clever Cryptography Could Protect Privacy in Covid-19 Contact-Tracing Apps*, WIRED, https://www.wired.com/story/covid-19-contact-tracing-apps-cryptography/ (accessed Apr. 8, 2020).

10 This information will include the keys necessary to derive the rolling device identifiers and decrypt the metadata advertised by that user during the relevant time window. Apple/Google, Exposure Notification: Cryptography Specification v. 1.2, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.2.pdf (accessed Apr. 2020) [hereinafter Cryptography Specification]; Greenberg, *supra* note 6.; Whitaker & Etherington, *supra* note 5.

enabling functionality into their underlying operating systems. Removing the need to download an app widens the reach of the platform and would enable interaction with a broader ecosystem of apps and government health authorities.[11]

Based on initial specifications released by Google/Apple, the ENS framework will, together with associated apps, generate and collect four types of information:

1. Bluetooth identifier codes and associated contact event information: generated by the ENS and stored decentrally on individual devices.
2. Positive diagnosis information: uploaded to the app server by the user along with their associated contact identifiers ('diagnosed identifier codes').
3. Associated information: when an individual notifies via the app that they have the virus, their individual IP address and other metadata will be detectable by the app server.[12] Apple and Google currently require that apps using the ENS promise not to collect and retain this information.[13] 'Associated encrypted metadata' including information about the timing and proximity of relevant exposure events will be stored decentrally on user devices, and upon diagnosis, notification will be decrypted locally.[14]
4. Notifications to exposed users: the ENS will download and broadcast diagnosed identifier codes once per day. [15] The ENS will identify phones with matching codes and will employ an algorithm locally to assess the risk of exposure based on the de-encrypted associated exposure metadata. The ENS will share information with the app about how many alerts were generated and the dates of exposure events.[16] The app will then generate an exposure detection notification to users identified as at risk. At the time of exposure notification, the app server will receive additional information from matched users about the time and attenuation of exposure.[17] Apps may request or require additional information from users at the point of

11 Press Release, Apple *supra* note 2.

12 CBS This Morning Tracking the Virus: Apple and Google Partner Up, https://www.youtube.com/watch?v=N2It_DXnKg8&feature=youtu.be.

13 Cryptography Specification, *supra* note 10 at 10 (stating that servers "must not retain metadata from clients uploading Diagnosis Keys", ie notifying a positive diagnosis); *see also* Patrick Howell O'Neil, *Google and Apple ban Location Tracking in Their Contact Tracing Apps*, MIT Tech. Rev., https://www.technologyreview.com/2020/05/04/1001060/google-and-apple-lay-out-rules-for-contact-tracing-apps/ (accessed May 4, 2020) (describing the restrictions mandated by the technology companies for apps running on their system).

14 Bluetooth Specification, *supra* note 9 at 3–4 (received rolling proximity identifiers will be timestamped and the associated encrypted metadata broadcast by a device will include data about radiated transmit power levels for better distance approximation).

15 Apple/Google, Exposure Notification: Frequently Asked Questions v. 1.1, https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf (accessed May 3, 2020) [hereinafter FAQ].

16 *See* Cryptography Specification, *supra* note 10 at 6 (stating that server operators will not learn the identity or location of those recently in contact with diagnosed user). It is not clear, however, if the app operator will learn any other information about devices receiving exposure notifications. See FAQ, *supra* note 15 at 3, 5–6) (stating that Apple, Google and other users will not have access to information shared by the ENS technology but that government health authorities will, subject to 'specific criteria around privacy, security and data control'.)

17 Bluetooth Specification, *supra* note 9 at 6 (app server receives a "detection summary" with the number of matches detected, dates of detection and requests further information from exposed users about day, duration

exposure notification. For example, exposed individuals may elect to upload their own unique identifiers to warn those with whom they may have been in contact.[18]

A potential fifth category of information would be a combination of the exposure data collected by apps using the Google/Apple ENS with individual user identities and location data in order to (i) assist law enforcement to ensure quarantine of infected and/or exposed individuals; (ii) use location data in aggregate to track the spread of the virus across a population; or (iii) use individual exposure data to make inferences about health such as a green light or 'all clear' indication that could be shared with third parties such as employers. Apple and Google have designed their system to make automated collection of this fifth category of data using their ENS prohibitively difficult.[19] However, those who administer apps using the system could collect some of this information separately at the time of diagnosis or exposure notification. Furthermore, it should be noted that Apple/Google's ENS has reserved functionality for additional unspecified associated metadata that might be collected later.[20]

PRIVACY AND DATA PROTECTION ANALYSIS

Is This Personal Data Under the GDPR or Relevant US Law?

GDPR: Is This Data Relating to an Identifiable Natural Person?

The information broadcast by devices and collected by the app should be considered personally identifiable information as defined by the GDPR. The GDPR defines personal data as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[21]

Any data stored on individual phones is information 'related' to an individual.[22] Although encrypted, the unique identifiers broadcast by the ENS could be linked to natural persons. For example, geolocation tracking systems already present on most user devices could reassociate the Bluetooth beacon identifiers with particular

and attenuation of contact); FAQ, *supra* note 15, at 2 (Digital exposure notifications "will enable public health authorities to contact and provide guidance to the [exposed] individuals.")

18 FAQ, *supra* note 15, at

19 See Alex Hern, *NHS in Standoff With Apple and Google Over Coronavirus Tracing*, The Guardian, Apr. 15, 2020.

20 Bluetooth Specification, *supra* note 9 at 4 (specifying that Byte 2 and Byte 3 of Associated Encrypted Metadata are reserved for future use).

21 GDPR Art. 4 (emphasis added).

22 Kirsten Bock et al., Data Protection Impact Assessment for the Corona App v. 1.6 46 Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. [hereinafter DPIA for the Corona App], https://www.researchgate.net/profile/Joerg_Pohle/publication/341041607_Data_Protection_Impact_Assessment_for_the_Corona_App_Version_16/links/5eaa6932299bf18b9587dc54/Data-Protection-Impact-Assessment-for-the-Corona-App-Version-16.pdf?origin=publication_detail (accessed Apr. 29, 2020).

devices.[23] Google itself operates some of the most ubiquitous of these trackers.[24] The encrypted beacon signals therefore most likely meet the GDPR definition of personal data, as they are information in relation to an 'identifiable' natural person.[25] The technology companies' promises not to track location data for the Bluetooth signals or access the Bluetooth contact information held on individual phones are helpful technological and organizational measures that minimize the burden on individual privacy and increase security of processing. However, as a matter of law, they do not disassociate the data completely and so the activities remain subject to the GDPR.[26] Similarly, associated apps receive diagnosis information linked to an individual IP address, and will receive individuated information about those in contact with infected persons.[27] If the agencies follow-up with in-person interviews, as is expected, they will have identifiable personal data on at least a subset of people potentially exposed to the virus.[28]

GDPR: Is This a Special Category of Data Concerning Health?

Information concerning health is a special category of personal data under the GDPR that triggers extra protections. COVID-19 diagnosis qualifies as information concerning health. Both the ENS and the app receive identifiers linked to individuals with a positive diagnosis. Whether the Bluetooth rolling identifiers by themselves constitute sensitive 'data concerning health' requiring extra protection under the GDPR is a closer question. The definition of 'data concerning health' includes data that reveal information about an individual's health status.[29] The purpose of collecting the Bluetooth identifiers is to determine virus exposure. Organizations would therefore be wise to treat this information as special category data under Article 9 of the GDPR.

23 Stuart Thompson & Charlier Warzel, *Smartphones are Spies. Here's Whom They Report to*, The Privacy Project: New York Times (Dec. 20, 2019). If an entity with access to this location data also 'eavesdrops' on the Bluetooth beacons they could link broadcast identifiers to individual devices through GPS tracking. If this entity also downloads the official app it will receive diagnosis keys that they conceivably could use to pinpoint and identify infected individuals. See, eg https://github.com/DP-3T/documents/issues/169

24 Thompson & Warzel, *supra* note 23.

25 DPIA for the Corona App, *supra* note 22 at 47 ("The question of whether the operator of the app or the operator of the server can access the encrypted or pseudonymized data is irrelevant in terms of whether personal data are processed . . . . In order for the processing of personal data to be confirmed, it is sufficient for the TempIDs to be generated on the user's terminal equipment. The fact that the tokens are sent in encrypted form via a secure network does not change the personal nature of the tokens. Even with encrypted personal data, the personal reference remains intact.")

26 GDPR Recital 26; Whitaker & Etherington, *supra* note 5 (admitting that even with the privacy controls Google and Apple could hack the system to obtain access to personal data).

27 *See* Andy Greenberg, *Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered,* WIRED, https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses/ (accessed Apr. 17, 2020).

28 *See* Jason Bay, *Automated Contact Tracing is Not a Panacea*, https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98 (accessed Apr. 11, 2020) (explaining that effective contact tracing requires follow-up contact and oversight with a human).

29 GDPR Art. 4.

GDPR: Is the Data Anonymized or Pseudonymized?

Apple and Google claim that user data broadcasted through their ENS has been 'anonymised' by virtue of deidentification and decentralization.[30] However, anonymization is a moving target legally. The European Data Protection Board ('EDPB')[31] has made it clear that true data anonymization is a very high bar and data controllers often fall short of actually anonymizing data.[32] Information is anonymized, and outside of the reach of the GDPR, if, taking into account the means reasonably likely to be used, including the available technology at the time of the processing and technological developments, the information cannot be associated with a natural individual.[33] Recent research has demonstrated that a large range of techniques exist to re-identify individuals using seemingly anonymous information.[34] That more such technologies are being developed every day means that users can never be confident that data shared 'anonymously' will not be associated with them in the future. Data controllers equally cannot be sure that they will not be found liable for failing to protect de-identified data.[35] Perhaps for this reason, although Google and Apple claim the data processed through the ENS is 'anonymous', they have still instituted multiple controls to prevent re-identification in their design, in keeping with the GDPR's data minimisation and security of processing principles. These controls result in data that is at least *pseudonymized*. In contrast to anonymization, Article 4(5) GDPR defines pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." By implementing *pseudonymization* as a security of processing measure, data controllers can benefit from several relaxed standards under GDPR, including potentially processing for other compatible purposes pursuant to Art. 6(4)(e) GDPR.

For public health authority apps, these controls may render the ENS data fully anonymous. However, depending on how the apps are designed, the operating entities could collect personally identifiable information, such as IP addresses, in addition to

30 *See, eg* Whitaker & Etherington, *supra* note 5.

31 The European Data Protection Board (EDPB) is an independent body, tasked with ensuring consistent application of data protection rules throughout the European Union and promoting cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities.

32 *Guidelines of the European Data Protection Board 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak* § 2.2. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (accessed Apr. 21, 2020) [hereinafter *EDPB Guidelines 04/2020*].

33 GDPR Recital 46.

34 Alexandre de Montjoye et al., *Evaluating COVID-19 Contact Tracing Apps? Here Are 8 Privacy Questions We Think You Should Ask*, Computational Privacy Group, https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/ (accessed Apr. 2, 2020).

35 See, eg Class Action Complaint and Demand for Jury Trial, Dinerstein v. Google, LLC Case: 1:19-cv-04311 ¶¶ 5–6 (6/26/19) (claiming breach of data protection rules when a hospital shared de-identified patient records with Google, which held sufficient additional data to be able to re-identify the records).

the encrypted diagnosis keys generated by the ENS.[36] It is not possible to judge whether the apps process only anonymized information without analyzing the design of a specific app and understanding what information collection practices, such as manual contact tracing interviews or third party tracking, might be used alongside it.

Application of the GDPR

Based on the information currently available, automated notification of exposure using the ENS and associated apps is a personal data processing system subject to oversight under the GDPR. Article 24 of the GDPR mandates that data controllers, including joint controllers, implement appropriate technical and organizational measures to ensure and to be able to demonstrate that covered processing is performed in accordance with the Regulation.[37] All of the GDPR Article 5 principles, (i) lawfulness, fairness, and transparency, (ii) purpose limitation, (iii) data minimisation, (iv) accuracy (v) storage limitation, (v) integrity and confidentiality, and (vi) accountability, must be observed in the design and implementation of these systems.[38]

These principles translate into a specific architecture of protection and enforcement for data subjects. Articles 12–23 of the GDPR mandate clear 'pre-defined' rights for the data subject, including rights of access, rectification, and erasure. To ensure accountability, each Member State must empower a competent and independent supervisory authority to enforce the terms of the Regulations, including the power to investigate and impose fines and other penalties.[39] Controllers and processors must maintain records of processing activities, including the purpose for the processing, and ensure the processing is technologically and organizationally secure.[40] Controllers must also conduct specific impact assessments (Data Protection Impact Assessment or 'DPIA') including risk mitigation measures for processing activities that pose a high risk to data subject rights.[41] Data subjects themselves have the rights to lodge complaints with the supervisory authority, to seek judicial remedies and to receive compensation.[42]

Comparison with US Law: HIPAA and CCPA

By way of comparison, the application of US privacy laws such as the Health Insurance Portability Act (HIPAA)[43] Privacy Rule[44] or the CCPA of 2018[45] to a proximity

36 Apple and Google joint initiative on COVID-19 contact tracing technology, Ref. 2020/01 2–3, 11 (UK Information Commissioner Opinion, Apr. 17, 2020) (noting that it may be possible for app developers to process additional information, such as location data) [hereinafter ICO Opinion].

37 GDPR Art. 26 ("Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject [. . .] Irrespective of the terms of the arrangement [. . .], the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.").

38 GDPR Art. 25.

39 GDPR Art. 52, 58.

40 GDPR Art. 30, 32.

41 GDPR Art. 35.

42 GDPR Art. 77–84.

43 Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, §§ 261–64, 110 Stat. 1936 (1996) ("HIPAA").

44 Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002).

45 Cal. Civ. Code §§ 1798.100–1798.199 ("CCPA")

tracking system is more limited. This lack of coverage might seem to encourage innovation, but there is a greater risk that the absence of comprehensive standards could undermine public trust and delay roll-out of contact tracing technology at a critical moment.

HIPAA's Privacy Rule applies only to data collected by health providers themselves, or businesses hired by health providers to process their data.[46] An individual's diagnosis from a diagnostic lab would, therefore, be subject to HIPAA's Privacy Rule, but a Bluetooth exposure proximity system such as the one designed by Google and Apple would seem to fall completely outside HIPAA's parameters.[47] In fact, the reality might be somewhere in between, because associated apps could depend on diagnosis validation from health care providers who are subject to the HIPAA Privacy Rule.[48] However, as long as it is the individuals themselves who disclose health information to the ENS, and not the health provider directly, HIPAA would most likely not apply to the system.[49] This regulatory gap might provide an opportunity for experimentation and market competition for anyone to create virus tracking apps using GPS location data, Bluetooth handshake signals, or other personal biometric or commercial data.[50] However, in a national emergency, increased business experimentation is a dubious virtue.[51] A proliferation of products, some less reliable and trustworthy than others, could undermine adoption of reliable notification systems.[52] Furthermore, those whose participation is most important, health providers and public health agencies, may hesitate to share information (such as COVID-19 diagnoses) in machine readable formats without

46 HIPAA § 262(a); Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59,918.

47 Carmel Shachar, *Protecting Privacy in Digital Contact Tracing for COVID-19: Avoiding a Regulatory Patchwork*, Health Affairs Blog, https://www.healthaffairs.org/do/10.1377/hblog20200515.190582/full/ (accessed May 19, 2020) (stating that HIPAA's protections would not apply to Apple and Google's ENS). One workaround would be for a covered entity under HIPAA to 'hire' the Google/Apple system to provide Bluetooth handshake data to an app run by the covered entity. This would require a detailed processing agreement be put in place setting out the rights and obligations of the parties and the rights and remedies of data subjects. It is not clear, however, that either Google or Apple can or would agree to run the system under the direction of outside health care providers.

48 *See* Whittaker & Etherington, *supra* note 5 (stating that the Apple and Google are depending on public health providers to perform validation of user positive cases); Letter from Andrea Jelinek, Chair EDPB to Olivier Micol, Head of Unit European Commission DG for Justice and Consumers, April 14, 2020 (advocating that providers give patients a one-time code confirming a positive diagnosis that could be scanned into the app to ensure the information given to the app is correct and reliable).

49 See HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services, Box 4 "Surveillance Project", https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm (accessed Apr. 11, 2003).

50 *See, eg* Jennifer Huddleston, *Data Protection and the Pandemic: What We Can Learn for Future Policy,* American Policy Forum, https://www.americanactionforum.org/insight/data-protection-and-the-pandemic-what-we-can-learn-for-future-policy/#ixzz6M32djYX8 ("Policymakers should consider that the consequences of stringent data protection regulation might prevent other benefits including the potential innovative responses to emergencies like COVID-19") *but see* Ghose & Sokol, *supra* note 3 at 3 ("Technology platforms may hesitate to engage in tracking without official protection from liability under existing data protection regimes.").

51 *Cf.* Jack Morse, *North Dakota Launched a Contact-Tracing App. It's Not Going Well,* Mashable UK, https://mashable.com/article/north-dakota-contact-tracing-app/?europe=true (accessed May 7, 2020) (describing technical problems with a "home-grown" contact tracing app designed by a small company in North Dakota).

52 See Mobile Applications to Support Contact Tracing in the EU's Fight Against COVID-19 eHealth Network Common Toolbox for Member States, v. 1.0 16, 20–21 (Apr. 15, 2020) (EC) (advocating common EU standards for app performance and interoperability).

assurances that other system users are engaging in privacy protective practices.[53] The lack of protection could delay uptake by US health authorities and providers at the moment when such involvement is most needed.

The reach of the CCPA is also limited. CCPA is a consumer protection statute. By its terms, it excludes data covered by the HIPAA Privacy Rule and other state laws concerning the privacy of medical information.[54] Furthermore, the CCPA does not apply to information collected by small businesses unless data brokerage is their principal business.[55] The CCPA also does not clearly state whether its obligations apply to personal information that has been pseudonymized.[56] The Bluetooth signals gathered by an ENS may qualify as 'de-identified' or anonymized information under the CCPA even if they would not under the GDPR.[57] Clarifying how these different exclusions and carve-outs apply to a virus tracking and notification system and associated apps is no small task.[58] The law lacks a specialized regulatory agency tasked with its interpretation that can issue necessary guidance in a crisis. Finally, even if the law applied to a proximity notification system or associated applications, it would not necessarily prevent the use or sale of individual data collected through these systems for other purposes unless the user objected.[59] By prioritizing individual notice and opt-out over shared principles, the law requires more engagement by individuals at a moment, such as the point of diagnosis with a serious illness, when they are not well-equipped to provide it.[60] Any uncertainty patients and health providers have about how health information shared with third party applications could be used in the future may disincentivize use of the app. Lack of clarity about potential liability may cause companies to shy away from participating in the system.[61] Individuals may hesitate to share diagnosis information without assurances that their illness history and any associated health, contact, and lifestyle information will not be shared broadly in a way that could draw unwanted attention or impact employment, credit scores, or insurance

53 FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency, U.S. Department of Health and Human Services Office of Civil Rights 5–6, https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf (accessed Mar. 20, 2020) (permitting covered providers under HIPAA to provide 'telehealth' care using electronic communication products but encouraging providers as evidence of good faith to seek out reputable services that use stronger security and provide assurances that they will comply with HIPAA standards for business associates).

54 CCPA § 1798.145(c).

55 CCPA § 1798.140(c).120.

56 Data Guidance & Future of Privacy Forum, Comparing Privacy Laws GDPR v. CCPA, at 16, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

57 CCPA, § 1798.140(h).

58 *Cf.,* Pymnts, Deep Dive: How US Data Regulation Fragmentation is Affecting Merchants, Consumers, https://www.pymnts.com/news/regulation/2020/deep-dive-how-us-data-regulation-fragmentation-is-affecting-merchants-consumers/ (accessed Mar. 31, 2020) (describing the difficulty for US merchants in determining how and whether the patchwork of state privacy laws apply to their activities).

59 CCPA § 1798.120.

60 *See* Frank Pasquale, *Redescribing Health Privacy: The Importance of Information Policy*, 14 Hous. J. Health L. & Pol'y 96, 96–97 (2014).

61 *See, eg* Ghose & Sokol, *supra* note 33 at 3 ("To enable effective coordination between public and private sectors, government has to provide assurances to technology platforms, telecom providers, and tech firms that such may hesitate to engage in tracking without official protection from liability under existing data sharing will be exempt from any adverse regulatory action or private lawsuits, now or later.").

rates.[62] Meanwhile, widespread immediate adoption of the technology may be crucial for its success in containing spread of the virus. Even if adoption is widespread, damage to fundamental rights of privacy and security of individuals from unregulated sharing could linger for years.

What is the Lawful Basis for Processing?

When a contact tracing ENS, or associated app, falls within the GDPR's governance, processing of personal data must have a 'lawful basis', and processing of personal data concerning health must meet further 'lawful basis' thresholds. The *public/private* collaborations envisioned by digital COVID tracking systems raise interesting questions in this regard. Public health and disaster response functions are typically overseen by democratically accountable public agencies. But here private, commercial tech companies are getting involved—either as initiators, partners, or organizations picking up outsourced tasks. Understanding the scope and purpose under which public and private entities may perform these functions will be crucial for complying with the 'lawful basis' requirements in the GDPR. It will also be crucial for public trust.

Apple and Google have presented their ENS technology as a public-spirited and voluntary effort to assist in a time of crisis. This characterization may be reasonable. Nevertheless, Apple and Google are commercial entities accountable in governance and operation to profit-minded shareholders. In China, where Alipay and WeChat hosted the Health Code app used to track coronavirus exposure, those companies have asserted rights contractually to keep the data once the crisis is over.[63] One German technologist lamented to Reuters that it was a less than ideal solution to have large private technology platforms in control of the architecture holding 'all the contacts plus the medical status of citizens around the world . . . .'[64] At the same time, others are similarly wary of authoritarian governments and their law enforcement apparatus having unfettered access to such information.[65] The risk of 'function creep' and use of data for purposes unintended by the data subjects exists whether the government or private entities collect this data.[66]

The GDPR's insistence on a lawful purpose for processing, while not an absolute structural safeguard, can help to hold organizations legally accountable for the uses they make of data. Article 6 of the GDPR requires organizations to have a legal basis

62 Pasquale, *supra* note 60 at 105–113.

63 Remarks of Ruipeng Lei, Huazhong University of Science and Technology, Wuhan, China, Beyond the Exit Strategy: Ethical Uses of Data-Driven Technology in the Fight Against COVID-19, Nuffield Council on Bioethics and Ada Lovelace Institute Webinar, https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19 (accessed Apr. 17, 2020).

64 Douglas Busvine, *German Tech Startups Plead for European Approach to Corona Tracing App*, REUTERS, https://www.reuters.com/article/us-health-coronavirus-tech-germany/german-tech-startups-plead-for-european-approach-to-corona-tracing-app-idUSKCN21W20F (accessed Apr. 14, 2020).

65 *See* Baker, *supra* note 3; Valentino-DeVries, *supra* note 1.

66 Remarks of Lynette Taylor, Beyond the Exit Strategy: Ethical Uses of Data-Driven Technology in the Fight Against COVID-19, Nuffield Council on Bioethics and Ada Lovelace Institute Webinar, https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19 (accessed Apr. 17, 2020).

for processing personal data.[67] In addition, Article 9 states that processing of special category data such as information concerning health is forbidden unless a specific exemption applies.[68] Organizations must therefore have a general lawful basis and a special category exemption lawfully to collect and analyze data concerning health. Any use of data, which exceeds what is necessary for the stated lawful basis, is prohibited by the GDPR unless it is covered by a separate permissible basis. A data controller needs only *one* lawful basis in each of Articles 6 and 9 as a 'floor', but it might choose to go above the floor. For example, the lawful basis for a public health authority's processing of data in a COVID-19 tracking app might be to protect the public from infectious disease. In addition, it might state that citizens have a choice whether or not to download or delete the app. The processing allowed by the GDPR is thus based on multi-dimensional limits that sometimes differ from what an individual considers appropriate protection. In contrast, the floor in notice-and-choice-based systems, such as the CCPA, depends on users individually setting boundaries as to what organizations can and cannot collect and for what purposes. If an individual is poorly informed, or for one reason or another is not a rational or fair decision-maker, the GDPR's approach is preferable.

COVID-19 Tracing Systems Have Multiple Controllers

The lawful basis that is open to a COVID-19 ENS under the GDPR will depend on the particular controllers involved. Each controller will need its own lawful basis. Under the GDPR, the data 'controller' is the entity that alone, or jointly with others, determines the purposes and means of the processing of personal data.[69] A data controller can be a private or public entity, but the lawful bases that each can rely upon differ.

Apple and Google's ENS could have multiple controllers. In May 2020, both companies released APIs that enable interoperability between Android and iOS devices using 'official' apps from public health authorities.[70] Second, in the following months, Apple and Google will enable a broader Bluetooth-based contact tracing platform by building this functionality into their underlying operating systems. These changes would enable interaction of the ENS platform with a broader ecosystem of apps (some of which might be offered by private entities) and government health authorities.[71] The purposes of those using the tracking technology are important for determining which lawful basis they may rely upon. They are likely to differ. For instance, public entities will have public functions that private entities do not.

67 GDPR Art. 6. The CCPA does not set a list of grounds that businesses must adhere to a priori to collecting, selling and disclosing personal information, and only provides for a posteriori mechanism, namely allowing customers to opt-out to the sale and disclosure of their personal information or to ask for erasure of the information.

68 GDPR Art. 9.

69 GDPR Art. 4.

70 Kari Paul, *Apple and Google Release Phone Technology to Notify Users of Coronavirus Exposure*, Guardian, May 20, 2020; Apple press release, *supra* note 2.

71 *Id*. Apple and Google have since clarified that "Only public health authorities will have access to this technology and their apps must meet specific criteria around privacy, security, and data control." FAQ, *supra* note 15 at 3. However, the situation is complex and still evolving. It's also possible that commercial entities can design workarounds once the functionality is embedded in the device operating system.

Lawful Bases for Public Health Agencies Managing Apps

The simplest cases under the GDPR involve apps managed by public health authorities. Apple and Google plan to limit access to the ENS to apps designated by a single public health authority in each state.[72] This section considers the lawful basis for processing carried out by a COVID-19 exposure app designed and managed by a public health authority.

While many people will consent to health systems using their data for the purpose of tracking exposure, the EDPB has emphasized that consent is not the optimal basis for public authorities.[73] Consent given to public authorities is generally not considered to be given freely due to the power or potential power of public agencies to compel compliance.[74] Users also may withdraw consent at any time, which could compromise the agency's public health mission if consent were withdrawn after notification of a positive diagnosis. Instead, the EDPB has clarified that public authorities should most likely rely on Article 6(1)(e) "necessary for the performance of a task carried out in the *public interest* or in the exercise of official authority vested in the controller."[75] An additional basis under Article 6 would also be subsection (1)(d) "to protect the *vital interests* of the data subject or of another natural person."[76]

Recital 46 of the GDPR states explicitly that both vital interests and the public interest are proper bases in the midst of humanitarian crises such as an epidemic:

> Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, *including for monitoring epidemics and their spread* or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.[77]

Where an app uses the Google/Apple ENS functionality and collects *additional* data (beyond proximity), such as user location, equipment details or subsequent health status, the public agency controller will need to evaluate such processing separately. Additional lawful bases may be required to justify it.[78]

Organizations also need a special category exemption in order lawfully to collect and analyze data concerning health. Article 9 provides for several exemptions for special category data relating to public health. Agencies using data concerning health could do so pursuant to Articles 9(2)(g) ('substantial public interest'), (2)(i) ('preventative medicine'), or (2)(h) ('public interest in the area of public health'.).[79] Many national health authorities are sufficiently empowered through their implementing or public

72 FAQ, *supra* note 15 at 3.

73 *See* Letter from Andrea Jelinek, to Olivier Micol, *supra* note 48 (stating that consent is not the most relevant basis for use of tracing apps by public authorities); *EDPB Guidelines 04/2020 supra* note 32 at ¶ 29 (stating that Art. 6(1)(e) task in the public interest appears to be the most relevant legal basis).

74 GDPR Recital 43.

75 EDPB *Guidelines 04/2020 supra* note 32 at ¶ 29; Letter from Andrea Jelinek to Oliver Micol, *supra* note 48.

76 *Statement of the European Data Protection Board on the Processing of Personal Data in the Context of the COVID-19 Outbreak* 2 edpb_statement_2020_processingpersonaldataandcovid-19_en (accessed Mar. 19, 2020) [hereinafter *EDPB Statement*].

77 GDPR Recital 45 (emphasis added).

78 ICO Opinion, *supra* note 36 at 11–13.

79 Interestingly, vital interests, while available as an exemption under Article 9, would probably not apply to contact tracing as in the Article 9 context it can be used only where the data subject is "physically incapable of giving consent." GDPR Art. 9(2)(c).

health regulations to process contact tracing data according to one of these special category conditions.[80] However, the EDPB has suggested that Member States may want to pass specific implementing legislation to promote voluntary use of the app and setting out functional requirements for its use.[81]

Even where consent is not relied upon as the 'lawful basis' under Articles 6 and 9 for processing, European authorities have been clear that voluntary use is an important safeguard under the GDPR.[82] The foundational 1980 OECD Principles on the Protection of Privacy, including the principles of Collection and Use Limitation, as well as Security Safeguards and Individual Participation, require that any use of personal data should be undertaken with the knowledge and consent of the data subject where possible.[83] Requiring explicit consent supports the autonomy and control of the data subject over their personal information as well as inherently limiting the type of data that can be collected and how long it is kept. As such, a consent requirement should be viewed as an 'organisational measure' under the GDPR that facilitates GDPR principles of data and storage minimization, and lawfulness and transparency of processing. Even though public authorities do not need consent as a lawful basis, the GDPR requirements for Privacy by Design and Default require that it be sought as a safeguard where possible.[84] User consent is also required under related legislation, such as the EU ePrivacy Directive, which protects individual data located on mobile devices from being accessed via mobile communication networks.[85] The articulation of these principles through legislation has caused designers of tracing and notification systems to prioritize voluntary use. In contrast, officials in China and Israel, for example, have imposed virus exposure tracing software automatically.[86] India's mobile app began as a voluntary tool, but the government recently mandated its use as a condition of returning to the workplace.[87] Such non-consensual tracking, as well as default sharing of data with

80 *Eg* Act on the Reform of the Communicable Diseases Law (Communicable Diseases Law Reform Act) Gesetz zur Neuordnung seuchenrechtlicher Vorschriften—(Seuchenrechtsneuordnungsgesetz—SeuchRNeuG) of 20 July 2000 art. 13, 16, 28(1), http://www.rki.de/cln_011/nn_226614/DE/Content/Infekt/IfSG/Gesetze/gesetze__node.html; UK National Health Service Act 2006 §§ 1, 1A(1), 1E, 2A(2), 2B, 253; *see also* UK Coronavirus Act 2020 Schedule 21 "Powers Relating to Potentially Infectious Persons" (setting out emergency screening and testing powers for public health officers).

81 Letter from Andrea Jelinek to Oliver Micol, *supra* note 48.

82 Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 4, https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7 (accessed Apr. 28, 2020); Guidelines 04/2020 *supra* note 32 at ¶¶ 8, 24, 31.

83 OECD Guidelines, *supra* note 4 at §2(7).

84 The GDPR also provides data subject the right to object to processing of their data on a public health or other Article 6 basis. GDPR Art. 21.

85 Council Directive 2002/58 art. 5(3) 2002 O.J. (L 201) 37 (EC) [hereinafter ePrivacy Directive]. As is the case under the GDPR, processing done on the basis of Member legislation that constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard public security may be undertaken without consent. ePrivacy Directive Art. 15. See also *EDPB Guidelines 04/2020 supra* note 32 at ¶¶ 10–13.

86 *See* Natasha Singer & Choe Sang-Hun, *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, NY Times (Mar. 23, 2020); Helen Davidson, *China's coronavirus health code apps raise concerns over privacy*, The Guardian (Apr. 1, 2020).

87 India Today, *Coronavirus Lockdown: No More Voluntary, Aarogya Setu App Now Mandatory for Office Workers*, https://www.indiatoday.in/technology/news/story/coronavirus-lockdown-no-more-voluntary-aarogya-setu-app-now-mandatory-for-office-workers-1673438-2020-05-01 (accessed May 1, 2020). The Ministry of Home Affairs has backed away from this stance and instead suggested that citizens use "best

law enforcement and national security services, greatly increases the risks that agencies may abuse their authority and use public health data for illegitimate surveillance, law enforcement, or targeting purposes.[88] For this reason, the Israeli Supreme Court recently barred the Israeli security service from continuing to access citizen mobile data for virus tracking without specific legislative authorisation.[89] Furthermore, the Court specified that even under such legislation, mobile tracking should be voluntary.[90]

Note, however, that if a system is 'voluntary' but does not depend on consent for a 'lawful basis' under Article 9 of the GDPR, controllers can define informed consent in a way that differs from the GDPR's definition of 'consent'. For example, information about choices may not be as specific and extensive (they might seek what is known as 'broad consent'), and some choices may be opt-out. Furthermore, controllers would not be obligated to provide the same automatic rights of withdrawal or erasure.[91] However, data subjects will retain other GDPR default rights, such as the to object to processing,[92] to rectify any inaccurate data held, and to seek associated legal remedies.[93]

Lawful Bases for Private Companies

Any company acting as a controller as part of the ENS, and arguably Google and Apple themselves in administering and updating the ENS, will be a separate 'data controller' from the public authorities discussed above and thus will need their own distinct lawful basis for processing under Articles 6 and 9. Other private companies are not *currently* expected to be involved as data controllers with the Apple/Google ENS. Commercial entities coming into contact with the ENS in its first phase will most likely be doing so as processors for these public health authority systems. For example, the national health services in the UK and Australia operating their own notification systems have contracted with Amazon and Microsoft for certain data storage and information

efforts" to use and install the app. *Privacy Activists Pleased as Centre Softens Stance on Aarogya Setu App*, New Indian Express, https://www.newindianexpress.com/states/telangana/2020/may/19/privacy-activists-pleased-as-centre-softens-stance-on-aarogya-setu-app-2145222.html (accessed May 19, 2020).

88 See, eg Privacy International, Israel's Coronavirus Surveillance is an Example for Others—of What Not to Do, https://privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do (accessed May 1, 2020); Singer & Sang-hun, *supra* note 86.

89 See Mayaan Lubell, *Israel's Top Court Says Government Must Legislate COVID-19 Phone-Tracking*, Reuters, https://uk.reuters.com/article/us-health-coronavirus-israel-monitoring/israels-top-court-says-government-must-legislate-covid-19-phone-tracking-idUKKCN2280RN (accessed Apr. 28, 2020).

90 *See* Onetrust Dataguidance, Israel: Supreme Court Issues Decision on General Security Services' Tracking of Technological Data, https://www.dataguidance.com/news/israel-supreme-court-issues-decision-general-security-services-tracking-technological-data (accessed Apr. 27, 2020.

91 GDPR Art. 7(3) & 17(1)(b) (providing rights of withdrawal and erasure when consent is the lawful basis for processing); *Cf.* Dept of Health and Social Care, Data Protection Impact Assessment NHS COVID-19 App PILOT LIVE RELEASE Isle of Wight 26 (May 6, 2020) (UK) [hereinafter UK DPIA] (for health service app relying on Art. 6(1)(e) public interest basis, a withdrawal decision by data subject will not remove pseudonymized personal data already uploaded to the 'backend' central server).

92 GDPR Art. 21.

93 GDPR Art. 16.

management tasks.[94] Processors act according to the instructions of the data controller and so do not need their own legal justification.[95] It is possible, however, that in the second phase of the rollout of the Google/Apple system, a greater variety of apps will be permitted to use the interface. A company running *an app* on the Google/Apple system could be a separate data controller. In addition, a public health agency in a Member State might delegate management of their system to a private company in such a way that it becomes a data controller, at least for some aspects of personal data management..[96] We consider first apps managed under the authority of private entities, and then the role of Apple/Google themselves.

To qualify for the public health-related bases set out in Article 6, such as vital interests or task carried out in the public interest, a commercial entity would most likely need to act in concert with and under the direction of public health authorities.[97] The GDPR is clear that there must be some basis in Member State or EU law that defines the nature of a 'public interest', 'vital interest', or 'legal obligations' for these bases to apply.[98] A private entity cannot just cloak itself in good intentions and claim to act for the public.[99] For example, Israeli spyware firm Group Technologies Ltd. ('NSO') , the firm suspected of helping the Saudi government track down dissident Jamal Khashoggi, is also marketing to various governments its software capabilities for monitoring individual virus exposure.[100] While such tracking might be broadly in the public interest during a pandemic, the GDPR requires some foreseeable basis in law before such an entity can purport to represent the public good. Recital 41 GDPR clarifies that "where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament [. . .] However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it." Private entities that exercise a clear public function, such as a university conducting medical research or a public utility, may also be able to rely on a public interest or official authority basis for processing if supported by law.[101]

Instead of a public interest basis, private companies could claim a 'legitimate interest' basis for processing exposure-related data, but, with exceptions, this will also require coordination with a public health authority or the agreement of the data subject. Article

94 UK DPIA, *supra* note 91 at 23; Aus. Department of Health, THE COVIDSAFE APPLICATION Privacy Impact Assessment 11, https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-covidsafe-application-privacy-impact-assessment.pdf (Apr. 24, 2020).

95 GDPR Art. 28 & 29.

96 *Cf.*, Morse, *supra* note 51 (North Dakota health authority partnered with local private company to deliver exposure tracking app).

97 GDPR Art. 6(4).

98 GDPR Recital 45.

99 *Id.* (stating that it would be for Member State law to determine whether and when a private entity could claim to act on the basis of a legal obligation or to further the public interest.)

100 Gwen Ackerman &Yaacov Benmeleh, *Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading*, Bloomberg, https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus (accessed Mar. 17, 2020).

101 GDPR Recital 45; *see* Data Protection Act 2018 ch. 12 (UK) Explanatory Notes § 8 ¶ ¶ 80, 85, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf (noting that a university may act as a public body when processing data for medical research).

6(1)(f) of the GDPR allows processing that is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject."[102] Third parties certainly have a legitimate interest in knowing whether they have been exposed to COVID-19. However, a private company controller must have a legitimate claim to be the appropriate entity to vindicate that third-party interest based on their relationship to the data subject. This could include some kind of affiliation with a public health authority that typically would conduct contact tracing. Other situations include an employer–employee relationship where a safe workplace is an expectation, or situations where data subjects are clients and infection exposure is a concern (eg clients of a gym).[103] Otherwise, the processing would be outside of the "reasonable expectations of data subjects based on their relationship with the controller" and therefore the rights of the data subject would likely override the third-party interest.[104] Furthermore, any processing permitted under this basis must be limited only to what is necessary and proportionate.[105]

An alternative basis for processing is where it is 'necessary for performance of a[n existing] contract' with the data subjects.[106] For this basis to apply, it would not be sufficient that the contract terms might allow tracking of exposure events, unless such tracking has a close and substantial link to the contract's main purpose.[107] Furthermore, tracking of exposure must be necessary to achieve the contract's purpose, and the data subject must have been informed that this processing would occur.[108] As an alternative, affirmative and informed consent can provide a basis for exposure tracking so long as the consent is given freely. [109]

All considered, it is likely that, absent an employment or other relevant and close relationship, commercial entities providing tracking architecture through an app must either act together with and under the supervision of a public health organization or obtain affirmative individual informed consent for the processing of infection exposure data.

As mentioned, Google and Apple themselves in administering and updating the ENS could be in a situation where they independently manage collection of exposure data and exchange of Bluetooth identifiers. In this case, they would also need to specify a lawful basis for this processing. It appears that Apple and Google are trying to take steps to minimize situations where they would qualify for ongoing duties of a data controller. The result of these steps is debatable. On the one hand, because

102 GDPR Art. 6(1)(f) (emphasis added).

103 GDPR Recital 47 (providing, as examples of 'a relevant and appropriate relationship between the data subject and the controller', situations where the data subject is a client or in the service of the controller).

104 *Id.*

105 UK Information Commissioner's Office, *What is the 'Legitimate Interests' Basis?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#what_counts (accessed May 23, 2020).

106 GDPR Art. 6(1)(b).

107 *See Guidelines 2/2019 of the EDPB on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects* at 8–9, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf (accessed Apr. 2019).

108 *Id.*

109 GDPR Art. 6(1)(a) & Recital 32.

the ENS stores data locally on individual devices, Google and Apple may claim that they themselves do not determine the purposes and means of processing or actually process any personal data. The GDPR defines a data controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[110] On the other hand, this definition does not require that entities store or physically process data to be a controller: determination of means and purposes of processing by others is sufficient.[111] Just as designers of algorithms that engage in automatic processing are still 'data controllers',[112] it could be claimed that by virtue of designing, updating, and operating the ENS, Google and Apple are either joint 'data controllers' or in a 'data controller-data processor' relationship with public health authorities.[113] If they are joint data controllers, Apple and Google should also specify the lawful basis underlying their design and management of the ENS. As stated above, notwithstanding good intentions, these technology platforms would most likely need to rely on affirmative consent. It is unlikely that broad contact tracing, undertaken without regard to the services Apple and Google typically provide, would qualify as 'legitimate interests' of those businesses within the 'reasonable expectations' of their customers or 'necessary for performance of a[n existing] contract' with the data subjects.[114] Furthermore, the ePrivacy Directive requires explicit consent for processing of data collected automatically via the operation of a publicly available electronic communication service.[115]

The notion of consent under the GDPR is more robust than consent as defined under the HIPAA and the CCPA. Under the GDPR, consent is only valid if it was given freely and in response to clear, plain disclosures devoid of unfair terms.[116] For special category data, such as data concerning health, enhanced consent requirements apply. These are discussed below.

Processing of Special Categories of Personal Data

A similar requirement for public oversight exists when special category data is involved. All of the conditions in GDPR Art. 9, which relate to processing data concerning health

110 GDPR Art. 26.

111 The European Court of Justice has taken a broad approach to this classification—for example a party may be a joint controller even where it does not have access to any personal data processed by the system. The parties also do not need to share equal responsibility for the processing to be considered joint controllers. Case C-40/17 Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, [2020] 1 C.M.L.R. 16.

112 Letter from Andrea Jellinek, Chair, EDPB to Sophie in't Veld, Member of the European Parliament, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf (accessed Jan. 29, 2020).

113 GDPR Art. 26 & 29.

114 *See EDPB Statement*, *supra* note 76 at 2 (stating that providers of publicly available communication services may only retain and use location data about subscribers if it is made anonymous or used with consent.)

115 ePrivacy Directive Art. 5(3), 6 & 9; *see also Opinion of the EDPB on the Interplay Between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities*, at ¶ 40, https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf (accessed Mar. 12, 2019).When Article 5(3) of the ePrivacy Directive provides that, as a rule, prior consent is required for the storing of information, or the gaining of access to information stored in the end-users device constitutes personal data, Article 5(3) of the ePrivacy Directive shall take precedence over Article 6 of the GDPR with regards to the activity of storing or gaining access to this information.

116 GDPR Art. 7 & Rec. 42; *see also* ePrivacy Directive Art. 2(f)(stating that consent by a user or subscriber under the ePrivacy Directive corresponds to a data subject's consent under the GDPR).

Table 1. Analysis of legal basis of processing for special category.

Subsection	*Processing Basis*	*Requirements*
9(2)(g)	Substantial public interest	Processing must be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for measures to safeguard the fundamental rights and the interests of the data subject.
9(2)(h)	Preventive or occupational medicine, medical diagnosis, . . . or . . . the management of health or social care systems	Data must be processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies.
9(2)(i)	Public interest in the area of public health	Union or Member State law must provide for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

for the substantial public interest, public health, or preventative medicine, require that such processing be undertaken 'on the basis of Member or Union law'.[117] Several of the Art. 9 conditions also impose additional substantive conditions (see Table 1).

Employers may process special category data under 9(2)(h) for the purpose of evaluating the working capacity of an employee, which might provide employers with an independent basis for conducting some form of targeted contact tracing. Processing necessary to carry out obligations in the field of employment and social security and social protection law is also allowed in so far as it is authorized by Union or Member State law.[118] This basis could allow employers and other commercial entities who have a defined social care function under local law to conduct some form of health care monitoring. Member States could also pass specific legislation or issue administrative guidance authorizing commercial parties without a social care function to manage an app or other architecture for contact tracing. That legal instrument could provide the basis for commercial entities offering tracing functionality such as Apple and Google

117 GDPR Articles 9(2)(g) ("substantial public interest"), (2)(i) ("preventative medicine"), or (2)(h) ("public interest in the area of public health.").

118 GDPR Art. 9(2)(b).

to claim to act according to one of the above special category conditions.[119] That same measure could establish governance and accountability mechanisms to ensure that private use of the data remains responsive to public concerns and democratic principles. Depending on the special basis employed, some processing may also require obligations of professional secrecy.[120] Note that even under the authority of such implementing legislation and professional secrecy, there is a strong argument that use of the app should still be voluntary to enhance public trust and to meet GDPR principles of privacy-by-default and privacy-by-design.[121]

Rather than a justification based on public interest reasoning or a special relationship of care, private entities processing data concerning health may rely instead on explicit consent. Enhanced consent requirements apply. The data subject will need to provide *explicit, informed consent* to the processing of personal data for each specified purpose.[122] Furthermore, under the GDPR, independent supervisory authorities are empowered to investigate any abuses as well as to ensure that rights to the data subject such as right of access, rectification, erasure, 'right to be forgotten' are respected.[123] By contrast, in the USA, the CCPA requires merely that businesses that collect personal information from California residents inform those consumers of the uses will be made of their data. Consent is not required; it is up to the consumer affirmatively to object. The HIPAA has consent requirements analogous to those found in the GDPR, but these only restrict covered health entities and their business associates. Other businesses, such as Apple and Google, which are not health care providers or insurers, may collect health data freely and need not seek consent if they obtain sensitive health-related data other than from a covered entity. Consent under the GDPR is therefore a substantial use limitation that can help ensure that information provided to apps will not be used to target or disadvantage users. In the USA, where consent does not provide firm limitations, a recent poll found that nearly three in five people would not be willing to download and use an infection-tracing app largely due to mistrust of tech companies and their willingness to safeguard privacy.[124]

119 *Cf.* John Timmons & Tim Hickman, COVID-19 and Data Protection Compliance, White & Case, https://www.whitecase.com/publications/alert/covid-19-and-data-protection-compliance (accessed Mar. 26, 2020) (stating that private organizations that act on the advice of medical advisors or public health authorities may be able to claim public interest in the area of public health or preventative medicine as a basis for processing COVID-related personal data). Such legislation could also provide a basis for collecting data directly from devices under the ePrivacy Directive Art. 15. See *EDPB Guidelines 04/2020 supra* note 32 at ¶¶ 12–13.

120 This is not necessarily a barrier for a commercial company. In the UK, professionals (and other people) owe duties of confidentiality whenever information has the quality of confidential information and a duty has arisen. A duty can arise where there is a reasonable expectation of confidentiality. Duties can also be imposed by contract, including by employment contracts.

121 Letter from Andrea Jelinek to Oliver Micol, *supra* note 48.

122 GDPR Art. 9.2(a).

123 GDPR Articles 15–22.

124 Craig Timberg et al., *Most Americans are Not Willing or Able to Use an App Tracking Coronavirus Infections. That's a Problem for Big Tech's Plan to Slow the Pandemic*, Wash Post ("A major source of skepticism about the infection-tracing apps is distrust of Google, Apple and tech companies generally, with a majority expressing doubts about whether they would protect the privacy of health data"), https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/ (accessed Apr. 29, 2020).

CONCLUDING REMARKS

The GDPR is known to have an expansive scope. COVID-19 app tracking systems are likely to fall within its purview, unlike narrower sector-specific rules such as the US HIPAA, and even the new CCPA. Counter-intuitively the scope of the GDPR is not likely to be a hindrance, but rather an advantage in conditions of uncertainty.

The principles in the GDPR offer a ready-made functional blueprint for system design that is compatible with fundamental rights. The principles are flexible enough to accommodate either a centralized system run under the auspices of a public authority, or a completely decentralized system designed by private entities with user consent. The utility of any ENS will depend on the reliability of diagnosis information and the broad availability of testing once notified of exposure. With these complementary capabilities, exposure tracing and notification is a proportionate response to the coronavirus public health threat that justifies some intrusion on the privacy rights of individuals.

Each system—decentralized processing by private entities or more centralized tracing overseen by public health agencies—has privacy advantages and disadvantages. Public health bodies are, at least in theory, more democratically accountable. On the other hand, users have, at least in theory, more robust rights to withdraw from commercial systems operating based on user consent. Combining both approaches is also possible. It will be important for data protection authorities closely to monitor either type of system to protect against function creep. In addition, each jurisdiction may choose to promulgate official regulations, legislation, or orders that set out the rights and obligations of all parties involved in contact tracing even when users consent. These provisions could include requirements that the data not be kept, except in aggregate form, after the public health crisis.[125] It will also be helpful to involve civil society organizations and ensure representation of groups such the elderly, minors, the incarcerated, etc to provide oversight and advice on use of the technology.[126] This is in keeping with the GDPR's mandate to ensure 'lawfulness, fairness and transparency' in processing.[127]

ACKNOWLEDGEMENTS

The authors thank David Erdos and anonymous reviewers for their helpful comments. The authors acknowledge the support by the Novo Nordisk Foundation for the scientifically independent Collaborative Research Program for Biomedical Innovation Law (grant NNF17SA0027784).

125 Letter from Andrea Jelinek to Oliver Micol, *supra* note 48.

126 Taylor, *supra* note 66.

127 GDPR Art. 5(a).